DEPARTMENT OF THE NAVY
FLEET AVIATION SPECIALIZED OPERATIONAL
TRAINING GROUP PACIFIC FLEET
P.O. BOX 357068
NAS NORTH ISLAND
SAN DIEGO, CALIFORNIA 92135-7068

FASOTRAGRUPACINST 5239.1B
N01C
05 JUN 1995

FASOTRAGRUPAC INSTRUCTION 5239.1B

Subj: AUTOMATED INFORMATION SYSTEMS SECURITY

Ref: (a) FASOTRAGRUPACINST 5530.1C
(b) COMNAVTELCOM AIS Security Guidelines of 1 Dec 90
(c) COMNAVAIRPACINST 5239.2A
(d) COMNAVAIRPAC Security Handbook
(e) OPNAVINST C5510.93E
(f) OPNAVINST 5510.1H

Encl: (1) Personally Owned Systems
(2) System Accreditation
(3) Interim Authority To Operate (IATO)
(4) Processing Classified Material
(5) Software
(6) Telecommunication
(7) Compact Disks

1. Purpose. To promulgate requirements for security of computer systems' hardware and software, including major components, peripheral equipment, cabling, systems and application software, and data. This instruction does not cover other types of electronic equipment or printed copy of computer generated data. Security of such material is covered by reference (a).

2. Cancellation. FASOTRAGRUPACINST 5239.1A

3. Objective. The intent of Automated Information Systems Security (AISS), herein referenced interchangeably with Automated Data Processing Systems Security (ADPSS), is to ensure the availability of reliable information and automated mission support. This requires a fine balance between user friendliness and strict control over hardware and software. The Commanding Officer draws upon advice of staff experts and will determine the ideal balance between information and control based on the unique needs of the command. The Commanding Officer is dedicated to an effective Information Security program including but not limited to the prevention of illicit reproduction of copyrighted software, security of sensitive and classified data, prevention of unauthorized use or misuse of information systems, and physical security of AIS assets. Reference (b) provides detailed guidelines on the application of AISS concepts to operating environments.

4. Scope. This instruction covers all facets of nontactical information processing at Fleet Aviation Specialized Operational

Training Group, Pacific Fleet. Embedded systems are excluded from coverage. This instruction should be used as a basis for Detachment AISS instructions. In the event of conflict with guidance provided by higher level directive (e.g., reference (c)), that guidance will prevail.

5. Organization.

a. The Commanding Officer is the Designated Approving Authority (DAA) for Headquarters. DAA authority and responsibility for detachment information systems security programs are hereby delegated to Officers-in-Charge of detachments.

b. The Automated Data Processing Security Officer (ADPSO) is appointed by the Commanding Officer in writing and is the senior staff resource for all matters dealing with automated information security matters.

c. Automated Data Processing System Security Officers (ADPSSO's) are appointed by the Commanding Officer in writing for each major system or group of computers in the command. These are typically collateral duties performed by an individual at the site of one or more computers serving similar functions. ADPSSO's are the on spot representatives of the ADPSO and are responsible for security of the system or systems for which designated.

d. Local area network (LAN) administrators are appointed by the Commanding Officer in writing for each local area network in the command. They are responsible for the overall management of the LAN, including system resources, operating and application software, user training, etc.

e. Network Security Officers (NSO's) are appointed by the Commanding Officer in writing for each local area network in the command. They perform similar duties as ADPSSO's for a LAN, including control of all hardware, software, and data.

6. Action.

a. DAA.

(1) Appoint an ADPSO and provide for adequate training.

(2) Appoint other members of command AIS team, ensuring local coverage of all areas of the command in which information systems assets are located.

(3) Accredit systems for operation or approve Interim Authority to Operate (IATO).

b. ADPSO.

(1) Maintain an active, viable, and effective command Automated Information Systems Security Plan (AISSP).

(2) Ensure that all operating AIS's in the command have complete accreditation packages or have been provided an IATO.

(3) Maintain a viable training program, ensuring that each member and employee receives AISS awareness training before being permitted to access a system and at least annually, thereafter.

(4) Provide for AISS training of other members of the command information systems security team.

(5) Perform periodic inspections of all information system resources and practices.

(6) Report security violations, as appropriate.

(7) Maintain a copy of accreditation letters or IATO letters for all detachment information systems.

(8) Review all headquarters accreditation and IATO packages prepared by ADPSSO's and forward them to the DAA for final determination.

(9) Endorse requests for use of personally owned systems submitted in accordance with enclosure (1).

c. ADPSSO's.

(1) Enforce all security requirements in assigned area. This includes prohibition against eating, drinking, and smoking in vicinity of systems.

(2) Indoctrinate new system users in AIS concepts before they are permitted to use command assets. Maintain an ongoing sense of security awareness in assigned area.

(3) Investigate all AIS violations or incidents in the area to which assigned. Perform or assist in investigations in other areas, as directed. Report results of investigation to ADPSO.

(4) Endorse requests for use of personally owned systems submitted in accordance with enclosure (1).

(5) Complete accreditation packages or IATO's for all systems in accordance with enclosure (2) or (3).

(6) Ensure that all computer systems have appropriate logon banners indicating intended use, penalties for unauthorized use, citations, etc.

(7) Label all equipment to indicate the highest security level permitted to be processed.

(8) Provide "emergency backup" copy of system passwords in a sealed envelope to Legal Officer for safe stowage.

d. NSO's.

(1) Provide for backup of systems and application software. Advise LAN users regarding backup of their data.

(2) Jointly with Network Systems Administrator, maintain accounts of authorized users. Ensure user accounts are added and removed on a timely basis. Ensure propriety of password usage and change. Ensure system passwords are maintained in a sealed envelope in a secure place.

(3) Provide "emergency backup" copy of system passwords in a sealed envelope to Legal Officer for safe stowage.

e. All Hands.

(1) Ensure familiarity with the content of this instruction, particularly enclosures (4) through (7).

(2) Recognize that computer files (including but not limited to word processing documents, spreadsheets, databases, and locally generated program source code) are government assets and are not personal property.

(3) Use government computing assets only for official government business. This includes computers, printers, other hardware and peripherals, and software.

(4) Immediately report any AISS incidents to the area ADPSSO or ADPSO. In the case of a suspected virus, immediately halt all processing; do not turn off or reboot system.

(5) Adhere to a schedule and method for backups.

(6) Label all media with the highest security level of data contained thereon. Label all media with brief description of data contained (e.g., Official Letters, May 1993 through _____).

M. T. SERHAN

Distribution:
FASOTRAGRUPACINST 5216.2V (List A & B)

Personally Owned Systems

FASOTRAGRUPAC personnel who wish to use a personally owned computer system in government spaces will submit a written request, via the cognizant ADPSSO (as appropriate) and ADPSO, to the Commanding Officer. The request should briefly state the purposes for which the computer will be used and explicitly agree that all data files created on the computer will be compatible with government owned systems. The request should also declare that only unclassified material will be processed on the computer, that this instruction has been read and understood, that all government files created on the privately owned system are Navy property, and that the files will be transferred to government computers when the privately owned system is removed from FASOTRAGRUPAC spaces. The requestor will use his/her personal system only upon written approval of the request.

OTHER CONTROLS MAY APPLY.

System Accreditation

System accreditation is the process by which all known and projected variables are weighed and considered in light of threats, vulnerabilities, safeguards, and risks. Systems intended for processing of classified material must be certified in accordance with the requirements of enclosure (4). The accreditation package will be prepared by the ADPSSO assigned to the area in which the system will be located. The accreditation process will be performed in accordance with this enclosure and reference (d) and submitted via the ADPSO to the DAA.

The first step in the accreditation of a system is the identification of all significant hardware and software components of the system. This inventory (see Attachment (A) to this enclosure for an example) must describe each key piece of hardware, such as the central processing unit with keyboard and mouse, MODEM, printer, etc. Descriptions must include serial and plant property accounting numbers, brand and model identifier, key features, and a brief narrative description. Each separate cable need not be inventoried, but an adequate description of all key components must be included. Similarly, each piece of software must be identified; this means each package that was purchased for the system, e.g., MS-DOS ver 3.21, MS-Windows ver 3.1, WordPerfect ver 5.1, etc. Each separate disk file that collectively makes up the application need not be listed.

Next, determine the level of data that will be processed by the system. Submit a TVAR in accordance with the requirements of reference (e), as appropriate. Ensure those members/employees who will be using the system have appropriate clearances and that suitable personnel and physical controls are in place to prevent unauthorized access.

Further, each system must have a contingency plan. What will happen if a system component malfunctions? What if the entire system goes down? What effect will an environmental catastrophe have on the organization's operations and/or the command's mission? Is there a relationship with other units? What steps will be taken if a breach of security is suspected?

Finally, determine what physical safeguards may be available. Arrange for other necessary controls. Document all safeguards and environmental factors in the system area; e.g., overhead sprinklers and fire bottles, locked cabinets for pilferable material, locked office or classroom doors, safeguards from a variety of threats or vulnerabilities, limited access to base/building, secure storage for sensitive/classified material, etc. Test safeguards periodically.

The entire accreditation analysis will be thoroughly documented and submitted via the ADPSO to the DAA for certification. Certifications will be valid for a period of three years, unless a significant change is made to the system.

Sample Inventory

COMPUTER - Zenith model Z-248-50, 360Kb floppy drive, 1.44Mb floppy drive, 40Mb fixed disk, 1Mb memory, ser 123-456789, P/A# 09191-100001

PRINTER - Alps model P2000G, nine pin dot matrix, wide carriage, ser 234-567890, P/A# 09191-100002

OPERATING SYSTEM - MS-DOS v 3.21

APPLICATION SOFTWARE - WordPerfect v 5.1 (no serial #)
Lotus 1-2-3 v 2.3 (ser 22334455)
Ashton-Tate Dbase III (ser AT1234G)

(The form provided in reference (d) may be used for this purpose.)

Attachment A

Interim Authority to Operate

The DAA may grant Interim Authority to Operate (IATO) for systems that are undergoing the accreditation process. Minimum requirements for an IATO are a brief description of the intended use of the system, comprehensive inventory of associated hardware and software, and a detailed plan of action and milestones for the formal accreditation process. An IATO may be issued for a period not to exceed one year and may be for an individual system or a group of similar systems (e.g., several machines in a computer classroom).

An IATO should be prepared by the area ADPSSO and forwarded via the ADPSO to the DAA. The Authority takes the form of a statement signed by the DAA.

Processing Classified Material

Philosophy. Great care must be exercised in the operation of systems intended to process classified or sensitive information. DOS based computers generally don't have adequate safeguards to ensure that data is not inadvertently written to fixed disks, so extraordinary care must be exercised. The most effective way to control the accidental, unintended propagation of classified data is to use systems that have removable media. Not only should the data file be on an appropriately labelled floppy diskette, but the application program should be on a cartridge type of drive (e.g., Bernoulli or Syquest) or a removable fixed disk. Exercise suitable care in securing these removable media and the propagation problem will be minimized.

Labelling. All media should be labelled with the highest classification of material contained on it. Accordingly, separate media should be used for confidential, privacy act, sensitive, confidential, and secret material. All hardware components of a system must also be marked with the highest level of classification authorized to be processed on them. All printouts containing classified material must also be appropriately identified. Suitable control of all classified material must also be exercised in accordance with the requirements of reference (f).

Tempest. Processing of material at the SECRET level requires that systems be appropriately certified. Process these systems in accordance with the provisions of reference (e).

Software

Government Software. Each system in use in the command has an inventory of authorized software which has been acquired for use on it. Members and employees are prohibited from copying software from a system for which it was purchased to another system. The original of each piece of software is maintained in the Resources Management Department; labelled copies and software manuals are issued to end users. All hands should ensure continued security of the distributed software and manuals.

Viruses. Viruses, Trojan Horses, Worms, and similar afflictions are pieces of software that are engineered to cause havoc on computer systems. They are introduced through illegitimate means, frequently carried on games or other freeware or shareware. There have been circumstances, however, when factory shrink wrapped software has been found to be infected. All hands should screen all new software with an antivirus package (e.g., MacAfee's Scan program) before introducing it onto a government system. The Naval Computer Incident Response Team (NAVCIRT) Computer Security Toolbox also has a variety of software that can be used effectively.

Privately Owned Software. Personally owned software shall not be installed on government computers. There shall be no exception to this policy.

Shareware. This category of software is actually commercial, copyrighted software for which a brief (frequently, 30 days) opportunity is provided to freely evaluate an application before purchase. Use of shareware in FASOTRAGRUPAC will be permitted only upon explicit authority of Department Heads. Since this means of marketing provides ripe opportunity for transmission of viruses, ensure that an antivirus program is run before using the shareware. Whether or not the shareware is found to meet command requirements, ensure that it is removed by the end of the evaluation period.

Games. Use of games on government computers is prohibited. Since many packages, including MS-DOS and Windows, come bundled with games, exercise care to ensure that they are removed or files deleted upon installation. While they may not violate copyright laws, they are not considered "official use," and must be removed from all systems. This requirement is explicitly imposed by reference (c).

Telecommunication

Only official FASOTRAGRUPAC business will be conducted using computers and MODEMs. Normally, this communication will be with other Navy or government telecommunication facilities. Neither government equipment nor telephone lines will be used for communicating with recreational bulletin board systems or commercial services (CompuServe, Prodigy, etc.). Telecommunication is subject to monitoring at all times.

Compact Disks

Current regulations require that obsolete compact disks (CD's) be retained indefinitely. Their composition is potentially hazardous and no approved method of disposal has yet been authorized by Navy. Proper care should be taken to safeguard obsolete CD's that are classified.